Secure Coding Guideline

1. Purpose

   The purpose of the Secure Coding Guideline is to assist agencies with implementing a secure software development lifecycle for any programs or scripts used on State of Montana information systems

2. Policy

   The Secure Coding Standard applies to the following controls found within the Information Security Policy.

   a. Information Security Policy
      1. Identify
         - 1.7.12
      2. Protect
         - 2.9.7
         - 2.11

   b. Information Security Policy – Appendix A
      1. AU-2 AUDITABLE EVENTS
      2. AU-3 CONTENT OF AUDIT RECORDS
      3. AU-5 RESPONSE TO AUDIT PROCESSING FAILURES
      4. AU-7 AUDIT REDUCTION AND REPORT GENERATION
      5. AU-8 TIME STAMPS
      6. AU-9 PROTECTION OF AUDIT INFORMATION
      7. AU-12 AUDIT GENERATION
      8. CM-4 SECURITY IMPACT ANALYSIS
      9. CM-5 ACCESS RESTRICTIONS FOR CHANGE
      10. CM-9 CONFIGURATION MANAGEMENT PLAN
      11. IA-5 AUTHENTICATOR MANAGEMENT
      12. RA-5 VULNERABILITY SCANNING
      13. SA-3 SYSTEM DEVELOPMENT LIFE CYCLE
      14. SA-4 ACQUISITION PROCESS
      15. SA-8 SECURITY ENGINEERING PRINCIPLES
      16. SA-10 DEVELOPER CONFIGURATION MANAGEMENT
      17. SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

3. Recommended Best Practices

   a. Any code (compiled computer program or interpreted computer script) developed for the State of Montana will be reviewed for threats identified in the most current version of the Open Web Application Security Project (OWASP) Top 10 and the Common Weakness Enumeration (CWE)/SANS Top 25 Most Dangerous Software Errors publications. Any high or critical severity threats identified in the code will be eliminated or mitigated.

b. Code will be checked for errors and vulnerabilities throughout the development lifecycle. This will include both static and dynamic code analysis.
    1. Developers are expected to have knowledge of current code analysis standards and agencies should support ongoing training and skill development.
    2. Development teams should use up-to-date automated tools to scan the entire code base.
    3. Peer reviews should be conducted during development phases.

c. Any compiled computer programs developed for use on State of Montana systems should be signed with a valid signature from a trusted certificate authority (CA).

d. Any code developed for use on State of Montana systems will be listed as part of the software inventory in the appropriate System Security Plan. The System Security Plan is then reviewed by the Information System Security Officer and any programs or scripts in the inventory are approved by the System Owner as well as the Authorizing Official in accordance with the Risk Management Framework (RMF) Standard.

e. Code will be developed and tested on systems that have an approved logical or physical separation from operational systems.

f. Code will be tested during development using anonymized data that does not contain sensitive data.

g. Code will have associated documentation identifying at least the purpose of the code and security controls that will be used to satisfy NIST baseline controls (e.g., Identification and Authentication, Access Control, etc.) commensurate with the RMF categorization of the system (i.e., Low, Moderate, or High).

h. User IDs and passwords with access to sensitive data will not be embedded within source code. If user IDs and passwords are required to be embedded in the code (e.g., for licensing and registration), developers and system administrators must ensure these accounts have no other authorizations than their original purpose (i.e., enforce principle of least privilege).

i. Any actions the code performs against data being processed or stored on a State system must be auditable in accordance with the System Security Plan for that system.

j. State agencies will verify that the software assurance model used by vendors is in line with this guideline and documented in the System Security Plan for that system. Software assurance may be evidenced by one or more of the following examples:
    1. System Security Plan for the system being procured in accordance with State of Montana RFP language.
    2. The Body of Evidence if the system has an Authorization to Operate.

3. Third party security assessments.
4. Vendor published documents describing their software assurance model.
5. Interconnection Security Agreement or contract language between the vendor and the State of Montana.

4. Related Documents

Secure Coding Guideline Attachment A